

CLAIMS

What is claimed is:

- 1 1. A method of operating a processing system on a network, the method
2 comprising:
3 encrypting an identifier of a mobile device on a wireless network; and
4 using the encrypted identifier to validate a request from a service initiator
5 directed to the mobile device.
- 1 2. A method as recited in claim 1, further comprising maintaining a different
2 cryptographic key for each of a plurality of service initiators.
- 1 3. A method as recited in claim 2, further comprising using the same
2 cryptographic key for each service initiator in a second plurality of service
3 initiators.
- 1 4. A method as recited in claim 2, wherein said encrypting comprises selecting
2 and using one of the cryptographic keys to encrypt the identifier, the method
3 further comprising including the encrypted identifier in a request to a remote
4 processing system, based on a request from the mobile device.
- 1 5. A method as recited in claim 4, wherein said using the encrypted identifier to
2 validate a request from a service initiator comprises selecting and using one of
3 the cryptographic keys associated with said service initiator to validate the

4 request.

1 6. A method as recited in claim 5, wherein said method is performed by a proxy
2 server connected to the wireless network and to a wired network including the
3 service initiator.

1 7. A method as recited in claim 1, wherein said encrypting comprises:
2 hashing the identifier with a cryptographic key; and
3 including the encrypted identifier in a proxy request to a remote
4 processing system based on an initial request received from the mobile device.

1 8. A method as recited in claim 7, wherein said using the encrypted identifier to
2 validate a request from a service initiator comprises using the cryptographic key
3 to decrypt an identifier included in the request from the service initiator; and
4 determining whether the identifier in the request from the service initiator
5 corresponds to the mobile device.

1 9. A method of operating a processing system on a network, the method
2 comprising:
3 encrypting an identifier of a mobile device on a wireless network;
4 including the encrypted identifier in a proxy request to a remote
5 processing system on a network, based on a request from the mobile device; and
6 using the encrypted identifier to control handling of requests by a
7 plurality of remote processing systems on the network to provide information to

8 the mobile device.

1 10. A method as recited in claim 9, further comprising maintaining a different
2 cryptographic key for each of the plurality of remote processing systems.

1 11. A method as recited in claim 10, wherein said using the encrypted identifier
2 to control handling of requests comprises, for each said request by a remote
3 processing system, using one of the cryptographic keys corresponding to the
4 remote processing system to validate the request.

1 12. A method of operating a proxy on a network, the method comprising:
2 storing an association of service providers and cryptographic keys;
3 receiving a request from a mobile device, the request directed to a remote
4 server on the network;
5 using the stored association to identify a cryptographic key associated
6 with the remote server;
7 using the identified cryptographic key to encode an identifier of the
8 mobile device;
9 incorporating the encoded identifier into a proxy request; and
10 sending the proxy request to the remote server on behalf of the mobile
11 device.

1 13. A method as recited in claim 12, wherein said storing an association of
2 service providers and cryptographic keys comprises storing a unique

3 cryptographic key for each of a plurality of service providers.

1 14. A method as recited in claim 13, wherein the stored association specifies a
2 plurality of network addresses for at least one of the plurality of service
3 providers, and wherein said using the stored association to identify a
4 cryptographic key comprises identifying a cryptographic key associated with a
5 network address to which the request is directed.

1 15. A method as recited in claim 12, wherein said using the identified
2 cryptographic key to encode an identifier of the mobile device comprises hashing
3 the cryptographic key with the identifier of the mobile device.

1 16. A method as recited in claim 12, further comprising:
2 receiving a request from a service initiator on the network to push
3 information to a mobile device;
4 determining whether the stored association includes a cryptographic key
5 associated with the service initiator;
6 if the stored association includes a cryptographic key associated with the
7 service initiator, using said cryptographic key to decode a device identifier in the
8 request from the service initiator;
9 determining whether the decoded device identifier corresponds to the
10 mobile device; and
11 allowing the request from the service initiator to be fulfilled only if the

12 stored association includes a cryptographic key associated with the service
13 initiator and the decoded device identifier corresponds to the mobile device.

1 17. A method of operating a proxy on a network, the method comprising:
2 storing an association of service initiators and cryptographic keys,
3 including a plurality of cryptographic keys and one or more network addresses
4 associated with each of the cryptographic keys;
5 receiving a request from a service initiator on the network to push
6 information to a mobile device;
7 determining whether the stored association includes a cryptographic key
8 associated with the service initiator;
9 if the stored association includes a cryptographic key associated with the
10 service initiator, using said cryptographic key to decode a device identifier in the
11 request from the service initiator;
12 determining whether the decoded device identifier corresponds to the
13 mobile device; and
14 allowing the request from the service initiator to be fulfilled only if the
15 stored association includes a cryptographic key associated with the service
16 initiator and the decoded device identifier corresponds to the mobile client
17 device.

1 18. A method as recited in claim 17, wherein said using the identified
2 cryptographic key to encode an identifier of the mobile device comprises hashing

3 the cryptographic key with the identifier of the mobile device.

1 19. A method as recited in claim 17, further comprising:

2 receiving a request from the mobile device, the request directed to a

3 network address representing a remote server on the network;

4 using the stored association to identify a cryptographic key associated

5 with the remote server;

6 generating a proxy request based on the request received from the mobile

7 device, by using the identified cryptographic key associated with the remote

8 server to encode an identifier of the mobile device and incorporating the encoded

9 identifier into the proxy request; and

10 sending the proxy request to the remote server on behalf of the mobile

11 device.

1 20. A method of operating a proxy on a network, the method comprising:

2 storing an association of service providers and cryptographic keys,

3 including a plurality of cryptographic keys and one or more network addresses

4 associated with each of the cryptographic keys;

5 receiving a request from a mobile client device, the request directed to a

6 network address representing a remote server on the network;

7 using the stored association to identify a cryptographic key associated

8 with the remote server;

9 generating a proxy request based on the request received from the mobile

10 client device, by using the identified cryptographic key to encode an identifier of
11 the mobile client device and incorporating the encoded identifier into the proxy
12 request; and
13 sending the proxy request to the remote server on behalf of the mobile
14 client device.

1 21. A method as recited in claim 20, wherein said using the identified
2 cryptographic key to encode an identifier of the mobile client device comprises
3 hashing the cryptographic key with the identifier of the mobile client device.

1 22. A method as recited in claim 20, further comprising:

2 receiving a request from a service initiator on the network to push
3 information to the mobile client device;

4 determining whether the stored association includes a cryptographic key
5 associated with the service initiator;

6 if the stored association includes a cryptographic key associated with the
7 service initiator, using said cryptographic key to decode a client identifier in the
8 request from the service initiator;

9 determining whether the decoded client identifier corresponds to the
10 mobile client device; and

11 allowing the request from the service initiator to be fulfilled only if the
12 stored association includes a cryptographic key associated with the service
13 initiator and the decoded client identifier corresponds to the mobile client device.

1 23. A method of operating a proxy on a network, the method comprising:
2 storing an association of service initiators and cryptographic keys,
3 including a plurality of cryptographic keys and one or more network addresses
4 associated with each of the cryptographic keys;
5 receiving a request from a mobile client device, the request directed to a
6 network address representing a remote server on the network;
7 using the stored association to identify a cryptographic key associated
8 with the remote server;
9 generating a proxy request based on the request received from the mobile
10 client device, by using the identified cryptographic key to encode an identifier of
11 the mobile client device and incorporating the encoded identifier into the proxy
12 request;
13 sending the proxy request to the remote server on behalf of the mobile
14 client device;
15 receiving a request from a service initiator on the network to push
16 information to the mobile client device;
17 determining whether the stored association includes a cryptographic key
18 associated with the service initiator;
19 if the stored association includes a cryptographic key associated with the
20 service initiator, using said cryptographic key to decode a client identifier in the
21 request from the service initiator;
22 determining whether the decoded client identifier corresponds to the

23 mobile client device; and
24 allowing the request from the service initiator to be fulfilled only if the
25 stored association includes a cryptographic key associated with the service
26 initiator and the decoded client identifier corresponds to the mobile client device.

1 24. A method as recited in claim 23, wherein said using the identified
2 cryptographic key to encode an identifier of the mobile client device comprises
3 hashing the cryptographic key with the identifier of the mobile client device.

1 25. A method of operating a server, the method comprising:
2 receiving a request to provide first information to a mobile client device
3 on a wireless network, the request including an encrypted identifier of the
4 mobile client device;
5 sending the first information in response to the request, for
6 communication to the mobile client device; and
7 sending a request to push second information to the mobile client device
8 by including the encrypted identifier in the request to push the second
9 information to the client device, such that the encrypted identifier in the request
10 to push the second information is used to validate the request to push the second
11 information.

1 26. An apparatus comprising:
2 means for encrypting an identifier of a mobile device on a wireless

3 network; and

4 means for using the encrypted identifier to control action upon a request
5 from a service initiator to provide information to the mobile device.

1 27. An apparatus as recited in claim 26, further comprising means for
2 maintaining a different cryptographic key for each of a plurality of service
3 initiators.

1 28. An apparatus as recited in claim 27, further comprising means for using the
2 same cryptographic key for each service initiator of a second plurality of service
3 initiators.

1 29. An apparatus as recited in claim 27, wherein said means for encrypting
2 comprises means for selecting and using one of the cryptographic keys to
3 encrypt the identifier, the apparatus further comprising means for including the
4 encrypted identifier in a request to a remote processing system, based on a
5 request from the mobile device.

1 30. An apparatus as recited in claim 29, wherein said means for using the
2 encrypted identifier to control action upon a request from a service initiator
3 comprises means for selecting and using one of the cryptographic keys
4 associated with said service initiator to validate the request.

1 31. An apparatus as recited in claim 30, wherein said apparatus is a proxy server

2 connected to the wireless network and to a wired network including the service
3 initiator.

1 32. An apparatus as recited in claim 26, wherein said means for encrypting
2 comprises:

3 means for hashing the identifier with a cryptographic key; and

4 means for including the encrypted identifier in a request to a remote
5 processing system based on a request received from the mobile device.

1 33. An apparatus as recited in claim 32, wherein said means for using the
2 encrypted identifier to control action upon a request from a service initiator
3 comprises means for using the cryptographic key to decrypt an identifier
4 included in the request from the service initiator; and

5 means for determining whether the identifier in the request from the
6 service initiator corresponds to the mobile device.

1 34. A processing system coupled to a wireless network and to a wired network,
2 the processing system comprising:

3 a processor; and

4 a storage facility coupled to the processor and storing instructions which
5 configure the processing system to:

6 encrypt an identifier of a mobile device on the wireless network;

7 include the encrypted identifier in a proxy request to a remote

8 processing system on the wired network, based on a request from the mobile
9 device; and
10 use the encrypted identifier to control handling of requests by a
11 plurality of remote processing systems on the wired network to provide
12 information to the mobile device.

1 35. A processing system as recited in claim 34, wherein the processing system
2 further stores a plurality of cryptographic keys, including a different
3 cryptographic key for each of the plurality of remote processing systems.

1 36. A processing system as recited in claim 35, wherein said using the encrypted
2 identifier to control handling of requests comprises, for each said request by a
3 remote processing system, using one of the cryptographic keys corresponding to
4 the remote processing system to validate the request.

1 37. A proxy gateway connected to a wireless network and to a wired network,
2 the proxy gateway configured to provide a plurality of mobile devices on the
3 wireless network with access to a plurality of processing systems on the wired
4 network, the proxy gateway comprising:
5 a processor; and
6 a storage medium having stored therein instructions which configure the
7 proxy gateway to perform the method comprising
8 storing an association of service providers and cryptographic keys;

9 receiving a request from a mobile device on the wireless network,
10 the request directed to a remote server on the wired network;
11 using the stored association to identify a cryptographic key
12 associated with the remote server;
13 using the identified cryptographic key to encode an identifier of the
14 mobile device;
15 incorporating the encoded identifier into a proxy request; and
16 sending the proxy request to the remote server on behalf of the
17 mobile device.

1 38. A proxy gateway as recited in claim 37, wherein said storing an association
2 of service providers and cryptographic keys comprises storing a unique
3 cryptographic key for each of a plurality of service providers.

1 39. A proxy gateway as recited in claim 38, wherein the stored association
2 specifies a plurality of network addresses for at least one of the plurality of
3 service providers, and wherein said using the stored association to identify a
4 cryptographic key comprises identifying a cryptographic key associated with a
5 network address to which the request is directed.

1 40. A proxy gateway as recited in claim 37, wherein said using the identified
2 cryptographic key to encode an identifier of the mobile device comprises hashing
3 the cryptographic key with the identifier of the mobile device.

1 41. A proxy gateway as recited in claim 37, wherein said method performed by
2 the proxy gateway further comprises:
3 receiving a request from a service initiator on the wired network to push
4 information to one of the mobile devices on the wireless network;
5 determining whether the stored association includes a cryptographic key
6 associated with said service initiator;
7 if the stored association includes a cryptographic key associated with said
8 service initiator, using said cryptographic key to decode a device identifier in the
9 request from said service initiator;
10 determining whether the decoded device identifier corresponds to said
11 one of the mobile devices; and
12 allowing the request from the service initiator to be fulfilled only if the
13 stored association includes a cryptographic key associated with said service
14 initiator and the decoded device identifier corresponds to said one of the mobile
15 devices.